
Title: Conference on Formal Aspects of Security (FASec '02)

Author: Howard S. Marsh

Date: 31 December 2002

These reports summarize global activities of S&T Associate Directors of the Office of Naval Research International Field Offices (ONRIFO). The complete listing of newsletters and reports are available under the authors' by-line on the ONRIFO homepage: <http://www.ehis.navy.mil/onrnews.htm>, or by e-mail to respective authors.

TABLE OF CONTENTS

Summary
Invited Talks and Keynote Address
Formal Analysis of Security Protocols
Quantitative Approach to Protocol Analysis
Emergent Behaviors and the Implications for Information Assurance
Resource Monitors and Privilege Based Access Control
Conclusion/Finding
Contacts

Keywords

Authentication
Certificates
Complexity
Computer Science
Cryptography
Emergent Behavior
Formal Methods
Information Security
Reference Monitors
Statistical Analysis

Summary

The Formal Aspects of Computing Science (FACS) Specialist Group of the [British Computer Society](#) sponsored an international conference dealing with formal methods for analysis and evaluation of information security during 18 through 20 December 2002. The conference was held at Royal Holloway, University of London. It dealt primarily with the analysis and evaluation of protocols for authentication and validation of security certificates in an Internet environment, and covered the standard, well accepted threat models and protocols. The intent was to describe ongoing research related to the application of formal methods to prove the ability of the protocols to deliver required performance with respect to those threats and to identify weaknesses that could be exploited. However, several presentations also addressed considerations of a broader nature. Those included the following four interesting papers:

- statistical analysis to complement formal methods and to provide results that could characterize protocol performance in a more quantitative way;
- the need to consider complex interrelationships within a network that can give rise to emergent behaviors;
- resource monitors and the management of access based on privileges;
- an historical perspective on cryptography

The overall content and level of the presentations was well selected by the organizing committee. The invited papers were extremely interesting and informative, and the regular papers were similarly of high quality and well presented.

Formal proceedings will be published in hard copy and disseminated to the registered participants. Softcopy may also be available on the web site. Further information and updates may be found at: <http://www.sbu.ac.uk/menass/fasec/>

Additional information on FACS objectives, organization, and events can be found at the web site: <http://www.bcs-facs.org/>

Invited Talks and Keynote Address

The conference included program of invited talks and a keynote address as follows.

Authenticity Types for Cryptographic Protocols
Dr. Andy Gordon, Microsoft Research (UK)

Verifying the SET Protocol: Overview
Dr. Lawrence Paulson, Microsoft Research and University of Cambridge (UK)

Lifting Reference Monitors from the Kernel (Keynote Talk)
Prof. Fred Schneider, Cornell University (USA)

Critical Critical Systems
Prof. Susan Stepney, University of York (UK)

Analysing Security Protocols
Dr. Dieter Gollman, Microsoft Research (UK)

Cryptographic Challenges: the Past and the Future
Prof. Bart Preneel, Kath University of Leuven (Belgium)

TAPS: the Next Generation
Mr. Ernie Cohen, Microsoft Research (UK)

Formal Analysis of Security Protocols

A majority of the conference was devoted to this area. Presentations covered a wide range of formal analysis applications, including protocol performance, protocol modeling, intrusion detection, and resistance to denial of service.

Since formal analysis requires detailed definition of fundamental aspects of the problem being analyzed, one obvious limitation is that the analysis is directed totally to the defined threats, the defined objective functions, and of course the defined protocol being examined. As a result, the analysis results, while useful, are limited to those predefined aspects of the overall problem faced by the information assurance community. If a different threat or a different set of objectives were imposed, the analysis would have to be done again. Results obtained from the previous analyses would not necessarily be relevant. This was noted explicitly in several of the presentations.

In general, the approaches that were presented shared a common foundation in logical formalism to infer behavior of the protocols. This type of analysis produces results that either confirm compliance with the objectives of the protocol under attack by the defined threats or identify specific failures. An important limitation in this type of analysis, and therefore a constraint in the applicability of the result, is that it is conducted as a “stand-alone” analysis. That is, it treats the protocol and the threat as a single adversarial instance without also considering other processes that occur concurrently in the network. Other processes that could affect an analysis include protocol screening at firewalls, potential multiple levels of authentication, and interactions with other protocols used for “housekeeping” and management in a distributed computing environment. The inclusion of such concurrent, and possibly interacting, processes could be a valuable addition to a formal analysis of information assurance.

Quantitative Approach to Protocol Analysis

The paper titled “Analysis of Probabilistic Contract Signing” applied quantitative statistical analysis to the formal treatment of security protocols. The case study was a two-party negotiation that required an exchange of privileges and commitments in a way that was fair to both parties, relatively prompt, and with assured nonrepudiation. It considered a contract signing protocol that was a variant of the Ben-Or, Goldreich, Micali, and Rivest (BGMR) protocol, intended to combine fairness with timeliness and still assure nonrepudiation to some predetermined level of confidence. The approach involved the two parties and a neutral “judge” who could respond immediately to each input and could issue a decision once the satisfactory level of confidence is achieved. The model assumed a Markov decision process. That is, the probabilities are biased by the history of prior actions of each participant.

Results were interesting in that they provide quantitative measures of performance of protocols under varying objectives for timeliness and fairness and under different assumptions regarding the ability of the participants to communicate with one another and with the judge. This added another important element to the formal analysis of protocols, since it introduced a quantitative way to characterize time sensitivity as a factor in determining the success of the protocol.

Further information can be obtained by contacting the authors: Gethin Norman at gxn@cs.bham.ac.uk and Vitaly Shmatikov at shmat@cs.sri.com

Emergent Behaviors and the Implications for Information Assurance

Professor Susan Stepney of the University of York (United Kingdom) presented an invited paper entitled “Critical Critical Systems”. She explained that the second instance of the word “critical” referred to the importance of the system, and the first instance referred to the emergent behavior that is similar to a “critical phase transition” in physics.

Prof. Stepney’s paper was principally motivational and dealt with this important area at a very general level. She made the point that the interactive nature of the various protocols and nodes in a network would give rise to “phase transitions” much like the ones we observe when water freezes or when ferromagnetic materials are heated to a temperature at which they become paramagnetic. She did not deal specifically with the nonlinear, interactive properties of networks and the emergent behaviors that occur when networks are stressed by excessive demands for service or by incompatibilities between protocols and network quality of service (QoS) requirements.

Her group’s research in this area is just beginning, so she had no specific analyses or research programs to discuss. However, she is clearly focused on this area as an important one for future research, and she indicated that she has funding from European sources to build her program.

Additional information can be found at <http://www-users.cs.york.ac.uk/~susan/> or by contacting Professor Stepney at susan.stepney@cs.york.ac.uk

Resource Monitors and Privilege Based Access Control

Professor Fred Schneider of Cornell University (United States) presented an invited paper entitled “Lifting Reference Monitors from the Kernel”. This was an extremely well presented and interesting paper, and it motivated consideration of the use of resource monitors and privilege management as a tool to enhance real time, dynamic QoS management up to the application layer.

Professor Schneider gave a brief history of resource monitors and then discussed the advantages using in-line reference monitors that can have access to calls on a wider set of resources than monitors confined to the kernel. He addressed the use of in-line reference monitors to control access to computing resources based on privileges assigned to the program requesting a resource as well as the basic system specifications for allocation of resources. Further information can be obtained from Professor Schneider at fbs@cs.cornell.edu

Potential ability to use this type of reference monitor as a means to extend QoS management to the application layer seems attractive. In this case, one might replace access control based on “program” and “system” privileges by a more complex and near real time dependence on “program group”, “user group”, “current operational context”, and “system” privileges. This could allow the reference monitor to be “aware” of the service level agreement (or QoS contractual agreement) assigned to each class of user and application under the existing operational and network conditions. If the reference monitor could be used in this way, and if network and operational objectives and constraints could be provided, it might yield a mechanism for building total QoS management and control from the network layer up to the user layer in a way that is responsive to defined objectives and priorities. In other words, it could provide QoS policy management that is responsive to dynamically changing objectives and priorities and QoS control for end-user services based on those policies. This appears to be an attractive area of research in support of network centric operational capabilities.

Conclusion/Finding

This conference was well organized and executed. Attendance was mainly from European researchers, and US participation included only four delegates, three of whom presented papers. The invited papers were the most interesting and informative. The other talks varied from very detailed to very general discussions of ongoing research and gave a good perspective on the international interests and capabilities in this area.

An important benefit to attending the conference was the identification of specific opportunities for research that could be of value. Areas of interest include quantitative statistical analysis as an extension of formal methods, complexity theory applied to

distributed computing and networks, and QoS management and control through the use of resource monitors that cooperate with network management and control processes.

Contacts

Conference Organizers:

Dr. Ali Abdallah	a.abdallah@sbu.ac.uk
Dr. Peter Ryan	peter.ryan@newcastle.ac.uk
Prof. Steve Schneider	steve@cs.rhul.ac.uk

Invited Speakers:

Mr. Ernie Cohen	arnie.cohen@acm.org
Dr. Dieter Gollmann	diego@microsoft.com
Dr. Andy Gordon	adg@microsoft.com
Dr. Lawrence Paulson	LP15@cam.ac.uk
Prof. Bart Preneel	bart.preneel@esat.kleuven.ac.be
Prof Susan Stepney	susan@cs.york.ac.uk

Keynote Speaker:

Prof. Fred Schneider	fbs@cs.cornell.edu
----------------------	--

The Office of Naval Research International Field Office is dedicated to providing current information on global science and technology developments. Our World Wide Web home page contains information about international activities, conferences, and newsletters. The opinions and assessments in this report are solely those of the authors and do not necessarily reflect official U.S. Government, U.S. Navy or ONRIFO positions.

[Return to ONRIFO Newsletters](#)